计算机工程 2012, 38(2) 146-147 DOI: 10.3969/j.issn.1000-3428.2012.02.047 ISSN: 1000-3428 CN: 31-1289/TP

安全技术

基于口令的三方认证密钥交换协议

王明辉 [1,2]，王建东 [1]

(1. 南京航空航天大学信息科学与技术学院，南京 210016；2. 盐城工学院信息工程学院，江苏 盐城 224051)

摘要： 传统的三方认证密钥交换协议不具备前向安全性，难以抵抗不可察觉在线字典攻击。为此，研究简单三方口令认证密钥交换协议，分析其存在的安全漏洞并加以改进，提出一种基于口令的三方认证密钥交换协议。分析结果表明，与其他协议相比，该协议的执行效率和安全性较高。

关键词： mso-ascii-font-family: 'Times New Roman' 口令')" href="#">mso-bidi-font-size: 8.0pt">口令 公钥加密 密钥交换协议 不可察觉在线字典攻击 Diffie-Hellman可计算Diffie-Hellmanmso-ascii-font-family: 'Times New Roman' 假设')" href="#">mso-bidi-font-size: 8.0pt">假设

Three-party Authentication Key Exchange Protocol Based on Password

WANG Ming-hui [1,2], WANG Jian-dong [1]

(1. College of Information Science and Technology, Nanjing University of Aeronautics and Astronautics, Nanjing 210016, China; 2. School of Information Engineering, Yancheng Institute of Technology, Yancheng 224051, China)

Abstract: Most three-party authentication key exchange protocols are not security enough, and can not resist the undetectable online dictionary attack. Aiming at these problems, this paper proposes a three-party authentication key exchange protocol based on password. It analyses the vulnerability of the simple three-party authentication key exchange protocol, and proposes an improved security new protocol. Analysis result shows that, compared with the simple 3PAKE and the other protocols, the execution efficiency on calculation of the new protocol is better.

王明辉
王建东

Keywords: password public-key encryption key exchange protocol undetectable online dictionary attack Computational Diffie-Hellman(CDH) assumption

PubMed
Article by Wang, M. H.
Article by Wang, J. D.

收稿日期 2011-07-13 **修回日期** **网络版发布日期** 2012-01-20

DOI: 10.3969/j.issn.1000-3428.2012.02.047

基金项目:

江苏省盐城市科技发展计划基金资助项目(YK2009092)

通讯作者:

作者简介: 王明辉(1977－)，男，硕士研究生，主研方向：信息安全，密码学；王建东，教授、博士生导师

通讯作者E-mail: wmh@ycit.edu.cn

参考文献：

[3] 胡红宇, 李军义. 改进的基于口令的群密钥协商协议[J].计算机工程.2011, 37(3):132-133 浏览

[4] Lu Rongxing, Cao Zhenfu. Simple Three-party Key Exchange Protocol[J].Computers & Security.2006, 26(1):94-97

[5] Guo Hua, Li Zhoujun, Mu Yi, et al. Cryptanalysis of Simple Three- party Key Exchange Protocol[J].Computers & Security.2008, 27(1/2):16-21

[6] Kin Hyun-Seok, Choi Jin-Young. Enhanced Password-based Simple Three-party Key Exchange Protocol[J].Computers and Electrical Engineering.2009, 35(1):107-114

本刊中的类似文章

1. 陈军, 刘锋, 高伟.一种简单的口令基三方密钥交换协议[J]. 计算机工程, 2011,37(8): 112-114
2. 蒋凯, 关佶红.基于重启型随机游走模型的图上关键字搜索[J]. 计算机工程, 2011,37(3): 42-43,46
3. 张开练, 廖湖声, 苏航.XQuery语言Hotspot编译系统的支撑框架[J]. 计算机工程, 2011,37(24): 28-31
4. 齐庆磊, 张浩军, 王逸芳.一种通用可组合安全的快速密钥交换协议[J]. 计算机工程, 2011,37(20): 94-96
5. 王成良, 谢克家, 刘昕.多核图像处理并行设计范式的研究与应用[J]. 计算机工程, 2011,37(14): 220-222
6. 卞仕柱;王建东;任勇军;方黎明;夏金月.强安全高效的认证密钥交换协议[J]. 计算机工程, 2010,36(7): 136-138,
7. 罗永红, 陈特放, 张友生.SOG环境中工作流应用的服务重调度策略[J]. 计算机工程, 2010,36(17): 19-22
8. 曹锋.改进代理多重签名方案的安全性分析[J]. 计算机工程, 2010,36(17): 155-157
9. 刘进, 马梁, 刘忠训, 王雪松, 王国玉.基于随机Hough变换的零基线正弦曲线检测[J]. 计算机工程, 2010,36(15): 1-3
10. 孙克泉.RSA密码分析中分解大整数的判定算法[J]. 计算机工程, 2010,36(15): 142-144

文章评论

反馈人		邮箱地址	
反馈标题		验证码	3033